October 12, 2001

INSPECTOR GENERAL PLAN 7740.1

FIVE YEAR AUTOMATED INFORMATION RESOURCES MANAGEMENT PLAN

FOREWORD

The enclosed Plan will serve as the Office of Inspector General, Department of Defense (OIG, DoD), primary tool for managing, developing and using automated information and information technology over the next 5 fiscal years. Information is the main product of the OIG, DoD. The Plan will serve as a guide for developing a cost-effective automated information technology program that will improve the efficiency and effectiveness of the OIG, DoD, mission performance.

The Plan is a working document, to be updated annually and amended as circumstances, such as budget adjustments, permit or dictate. The Plan is developed in coordination with, and based on inputs from, the OIG, DoD, components. The decisions of the OIG, DoD, Senior Management Group may generate changes in the Plan. Please forward recommended changes to this document to the Office of Administration and Information Management, ATTN: Information Systems Directorate.

FOR THE INSPECTOR GENERAL:

Joel L. Leson
Director
Office of Administration
and Information Management

2 Appendices - a/s

1

TABLE OF CONTENTS

CHAPTER 5
FUTURE PLANS

APPENDICES

CHAPTER 1
PLAN INTRODUCTION

1.1.   Introduction. The OIG, DoD, Information Technology (IT) Management Plan (referred to as the Plan) is the organization's primary method for managing the development and use of information and information technology over the next 5 fiscal years, 2001 to 2005. The Plan defines the status of the Internal Information Technology Program in the OIG, DoD, and charts the path the program will follow based on documented requirements from the OIG, DoD, Component Heads. Development of this updated Plan provides for the effective, efficient, and economical management of IT in the OIG, DoD. The Plan serves as a "living" document that is readily adaptable to the ever-changing advances being made in the IT field. It additionally serves as an organizational resource for IT direction, program coordination, acquisition management, internal and external reporting, program oversight and documentation, and resource investment accountability.

1.2.   References. See Appendix A.

1.3.   Cancellation. This Plan supersedes IGDP 7740.1, *Five Year Automated Information Resources Management Plan,* November 17, 1999.

1.4.   Background. This update of the Plan incorporates reference a and takes into account the progress made to date in OIG, DoD, IT management. Of particular importance is the progress of DoD-wide and OIG, DoD, internal Business Process Reengineering (BPR) initiatives. The entire DoD is working to standardize data and information systems, where appropriate, as a function of the BPR methodology. The Secretary of Defense has appointed the Inspector General, DoD, as one of the Department's Principal Staff Assistants (PSAs) in this process.

1.5.   Purpose of the Plan

       a.   The purpose of the Plan is to support OIG, DoD, missions through continually improving IT management. This includes the effective, efficient, and economic management, acquisition and use of IT. The Plan describes the OIG, DoD, goals and objectives and the transition strategy for migrating from the current to a target information program. The Plan is a tool that ensures the proper interfaces with the Planning, Programming, and Budgeting System (PPBS), and that supports appropriate IT programs.

       b.   The Plan is essential to the accomplishment of the OIG, DoD, mission. The organization has implemented numerous IT initiatives that directly aid or influence the way work is accomplished within the OIG, DoD.

1.6.   Scope of the Plan. The Plan covers all IT and identifies IT that will enable the OIG, DoD, staff to perform its mission in an effective and efficient manner, particularly during a period of decreasing resources. The scope of the IT planning effort encompasses an examination of the total organization from all aspects with respect to IT needs and requirements in support of OIG, DoD, mission, goals, and objectives.

1.7.   Objectives. The objectives of the Plan are to:

       a.   Support the goals and objectives of the OIG, DoD.

       b.   Develop an overall OIG, DoD-wide, IT process and program that is driven by integrated information needs.

       c.   Integrate the BPR initiatives underway within the DoD, as appropriate.

       d.   Analyze and identify duplicative activities.

e.   Identify near and long-term information needs consistent with the OIG, DoD, mission.

f.   Define central IT activities.

g.   Define and prioritize OIG, DoD, IT requirements to provide a means for obtaining and producing the timely and accurate information needed by auditors, investigators, and others providing policy, oversight, and support to the DoD.

h.   Integrate the IT Plan with prioritized OIG, DoD, activities.

i.   Ensure long-range system solutions.

j.   Ensure that approved Federal and DoD standards are applied in designing, developing, and operating automated systems.

k.   Ensure that the OIG, DoD, complies with all laws and regulations concerning the protection of sensitive information and the privacy of individuals in accordance with reference b.

l.   Disseminate automated information system (AIS) management policies, strategies, standards, and procedures throughout the OIG, DoD.

m.   Provide a document for use by management in monitoring the OIG, DoD, IT program.

n.   Serve as an information base for audits and reviews of IT, including ongoing Plan monitoring and maintenance.

o.   Support DoD IT management goals.

1.8.   **DoD IT Management Goals**

a.   The OIG, DoD, has modeled its goal on those published in reference c.

b.   The DoD has set as its goals to:

(1)   Become a mission partner.

(2)   Provide services that satisfy customer information needs.

(3)   Reform IT management processes to increase efficiency and mission contribution.

(4)   Ensure DoD vital information resources are secure and protected.

1.9.   IT Program Goal. Provide a cost-effective IT program that will improve the efficiency and effectiveness of the OIG, DoD, within budget constraints and in compliance with Federal statutes and guidelines, the BPR Program, and DoD guidance.

a.   **Program Objective #1:** Ensure that OIG, DoD, information systems and resources (automated and manual) support the overall mission needs and priorities of the organization.

b.   **Program Objective #2:** Promote IT integration through an emphasis on standardization and/or compatibility of hardware, software, and data elements.

c.   **Program Objective #3:** Ensure information is secure and available to authorized users.

    d. **Program Objective #4:** Review and ensure compliance with guidelines.

    e. **Program Objective #5:** Ensure OIG, DoD, component involvement throughout the planning process.

    f. **Program Objective #6:** Continue implementation of DoD-wide systems.

    g. **Program Objective #7:** Rapidly deploy appropriate advanced technology to support the mission.

    h. **Program Objective #8:** Develop Information Systems Directorate (ISD), Office of Administration and Information Management (OA&IM), human capital.

CHAPTER 2
OIG, DOD, ORGANIZATIONAL OVERVIEW AND MISSION

2.1.   <u>Organizational Overview</u>. Reference d establishes the OIG, DoD, as an independent agency within the DoD. The OIG, DoD, is composed of an Office of the Assistant Inspector General for Auditing (OAIG-AUD), an Office of the Assistant Inspector General for Investigations (OAIG-INV), an Office of Administration and Information Management (OA&IM), an Office of Departmental Inquiries (DI), and an Office of Intelligence Review (IR). The OIG, DoD, operates with a headquarters in the National Capital Region and field elements located throughout the United States and Wiesbaden, Germany.

2.2.   <u>Mission</u>. The statutory mission of the OIG, DoD, is set forth in reference d and is further delineated in reference e. The mission of the OIG, DoD, includes:

    a.   Conducting, supervising, monitoring, and initiating audits, evaluations, and investigations relating to programs and operations of the DoD.

    b.   Providing leadership and coordination, and recommending policies for activities designed to promote economy, efficiency, and effectiveness in the administration of, and to prevent and detect fraud and abuse in, such programs and operations.

    c.   Providing a means for keeping the Secretary of Defense and the Congress fully and currently informed about problems and deficiencies relating to the administration of such programs and operations and the necessity for, and progress of, corrective action.

2.3.   <u>Goals</u>. The goals of the OIG, DoD, as stated in reference a, are:

    a.   We will contribute to improving DoD operations in support of mission objectives by promoting efficient, effective, and economical operation of the Department.

    b.   We will reflect the best in Government by directing our resources toward becoming a model organization within the DoD and reflecting excellence in all aspects of our business.

CHAPTER 3
EXTERNAL INFLUENCES AFFECTING INFORMATION SYSTEMS
WITHIN THE OIG, DOD

3.1. Business Process Reengineering (BPR)

a. The Secretary of Defense appointed the Inspector General, DoD, as the PSA for BPR issues affecting the audit, inspection, and investigation functions throughout the DoD. This includes, but is not limited to, functional process improvement and data standardization. Other DoD components are responsible for other functional areas. These functional areas and their respective PSAs are:

(1)   Finance--Comptroller of the DoD

(2)   Health--Assistant Secretary of Defense (ASD) for Health Affairs

(3)   Human Resources--ASD for Force Management and Personnel

(4)   Reserve Components--ASD for Reserve Affairs

(5)   Materiel Resources--ASD for Production and Logistics

(6)   Procurement--Under Secretary of Defense for Acquisition

(7)   Information Management--ASD for Command, Control, Communications and Intelligence (C3I)

(8)   Command and Control--ASD for C3I

(9)   Legal--DoD General Counsel

(10) External Liaison--ASD for Legislative Affairs

(11) Public Affairs--ASD for Public Affairs

(12) National Defense Doctrine and Policy--Under Secretary of Defense for Policy

(13) Joint Warfighting Plans and Operations--Chairman, Joint Chiefs of Staff

b. The DoD BPR objectives state that:

(1)   Mission requirements and functional economic analyses underpin all DoD programs.

(2)   Mission needs determine information production and availability; mission responses must not be bound by information supply.

(3)   Defense is a joint, multi-Service effort. Supportive information systems are to be constructed from standard, jointly used elements.

(4)   Information management is a process for improving the productivity of all information-related work. Although it uses computers, it is primarily focused on overall organizational effectiveness and productivity.

c. As the DoD emphasizes these principles by promulgating changes to its directives and instructions, the OIG, DoD, is updating implementing instructions in accordance with the DoD changes.

This will ensure the OIG, DoD, adheres to the BPR principles when planning and implementing AIS. The ISD, OA&IM, will give primary emphasis to using DoD-wide standards and systems whenever appropriate, and to managing information on an organization-wide basis, while meeting the near-term needs of the OIG, DoD, components.

3.2.   Leadership Changes. We expect changes in leadership as a result of the political process and will adapt to any changes in the Administration.

3.3.   Budget Influences. The funding available for DoD programs and the OIG, DoD, budget remain in a state of flux. Programming and budgeting for the rapidly changing, BPR-driven, DoD IT mandated standards and migration systems continue to be a major challenge. Established fiscal guidance for the outyears may not accommodate changing standards and requirements. The OIG, DoD, will continue to update requirements for program and budget submissions. However, during each execution year, funding constraints will determine which IT initiatives will be implemented.

3.4.   DoD Requirements. As noted in paragraph 3.1, above, the Secretary of Defense has designated PSAs for DoD-wide functions other than audit and criminal investigations. These PSAs are devising migration systems and data standards in such areas as procurement, personnel, inventory, etc. The ISD, OA&IM, must respond to these new standards as the PSAs implement the new systems. As a result, it often becomes necessary for these DoD-wide functional programs to receive priority attention when these systems are required to come online.

CHAPTER 4
MAJOR INFORMATION SYSTEMS INITIATIVES

4.1.   Operating System Enhancements. Based on the Plan, the ISD, OA&IM, continues to implement projects to support the mission of the OIG, DoD, through the modernization of the Agency's automation and communications infrastructure. The ISD, OA&IM, is updating all systems to *Windows 2000*.

4.2.   Application Systems Enhancements. The ISD, OA&IM, continues to develop application systems. It is upgrading to *Office 2000*. The ISD, OA&IM, provided guidance and direction regarding the use of the OIG, DoD, Internet and Intranet sites. The ISD, OA&IM, supported several commercial off-the-shelf software packages by working with functional points of contact to ensure that the operating environment is suited for the required software deployment.

4.3.   Customer Support Improvements. The Help Desk workload continues to grow, but the number of outstanding calls continues to drop.
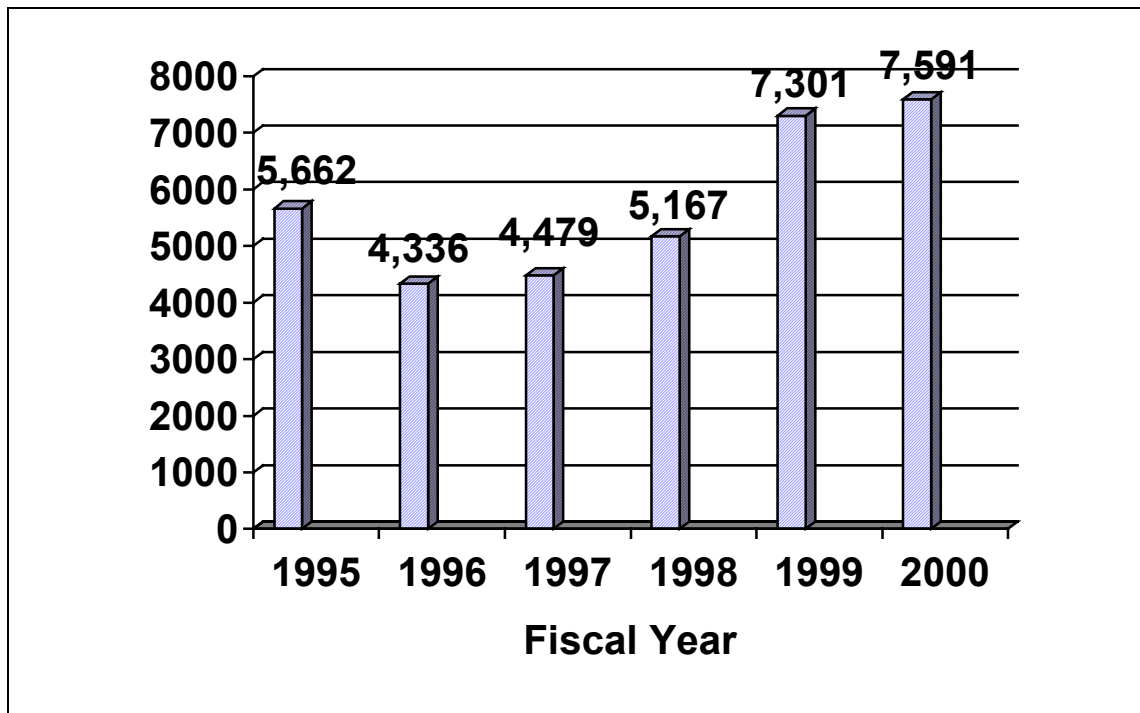

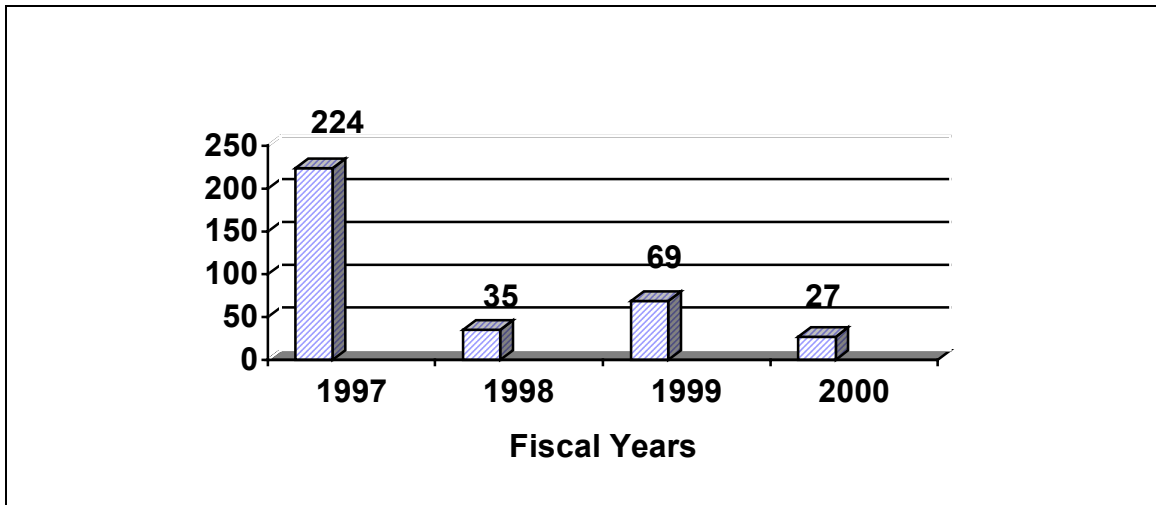Figure 1. Customer Support Calls for Fiscal Years 1995-2000

Figure 2. Customer Calls Carried from Previous Fiscal Year

4.4.   <u>Electronic Documents Records Management System (EDRMS).</u> The goal of this system is to provide the OIG, DoD, with an integrated system of electronic document and workflow management. In addition, the EDRMS will be consistent with the stated expectations of OIG, DoD, management. This includes collaboratively supporting the administration and Defense initiatives in a manner that imposes minimal burden on our customers and which is cost effective. This includes:

    a.   Minimally affecting other DoD initiatives and resources.

    b.   Reducing the burden on human resources supporting the records process.

    c.   Conforming to existing approved plans.

    d.   Eliminating funding redundancies.

4.5.   <u>Intranet/Internet.</u> The content of the OIG, DoD Web pages has been enhanced and reorganized to facilitate information retrieval. The ISD, OA&IM, and agency Web Authors continue to cooperate to enrich the content of the OIG, DoD, Intranet with information, pictures of the day, and *Toolboxes* to make the Website a more valuable tool which enhances the performance of the OIG, DoD, staff. This includes an updated Intranet menu, updated directorate Web pages, and Employee Council Web pages. The ISD, OA&IM, provides Web Authors with more advanced tools and training to produce Web pages. The OIG, DoD, is working to make its Web pages conform to privacy and handicapped access policies. Several applications that were previously server-based are being rewritten as Web-based to facilitate access.

4.6.   <u>Web-based Applications.</u> The ISD, OA&IM, is designing new Web-based application systems. This approach is being taken to improve:

    a.   Access to systems.

    b.   Mechanisms for deployment of applications, upgrades and revisions.

    c.   Overall report distribution.

4.7. <u>**Major Mission Support Actions.**</u> The ISD, OA&IM, procured notebook computers, scanners, and software licenses to support OAIG-AUD TeamMate customers. It also provided support to field offices, network capability, hardware, and software to support major investigations. The ISD, OA&IM, procured workstation computers to provide backup domain controllers for field activities. The minicomputer has been upgraded, and hardware continues to lifecycle out.

4.8. <u>**Defense Audit Management Information System (DAMIS).**</u> The ISD, OA&IM, is managing its portion of DAMIS to provide the entire DoD audit community a more effective tool for planning, coordinating, and exchanging information among the community and its customers. The project is ongoing. Recent achievements include:

   a. Movement toward Public Key Infrastructure (PKI) certification.

   b. A plan for system certification and accreditation.

   c. Completion of a follow-up module.

   d. Completion of *Versions one and two*.

   e. Completion of *Versions one and two* training.

   f. Plans for completion of updated versions and training on those versions.

4.9. <u>**Prevention of Inappropriate Use of Government IT Resources.**</u> The ISD, OA&IM, updated many policies to emphasize user responsibilities regarding protection and inappropriate use of Government resources. It participated in annual security briefings to educate users on the existence of these policies. It monitors E-Mail and Internet traffic to proactively keep the OIG, DoD, infrastructure problem free.

4.10. <u>**Upgrade of OIG, DoD, IT Infrastructure.**</u> The ISD, OA&IM, upgraded Frame Relay lines, routers, switches, servers, and network cabling. These initiatives improve access time to IT resources and provide a greater level of security.

4.11. <u>**Field Activity Support.**</u> The ISD, OA&IM, continues to visit field sites to provide support, identify needs, and give refresher training.

4.12. <u>**Disaster Recovery Operations.**</u> The ISD, OA&IM, continues to set up a location to provide offsite storage of backup information and a facility to provide continuing operations in case of an emergency that could cause unavailability of the OIG, DoD headquarters building's IT capability.

CHAPTER 5
FUTURE PLANS

5.1. Introduction. The following program objectives support the OIG, DoD, Goals and IT Program Objectives. Some actions (notably those under IT Program Objectives 3 and 4) will be accomplished in coordination with other elements of the OA&IM. All plans under Objective #3 will be modified and expanded by the Personnel and Security Directorate, OA&IM, which has been delegated prescribed IT-related information assurance duties by the Designated Approving Authority. On May 20, 1999, the Acting Inspector General promulgated a memorandum establishing a Senior Management Group. The decisions of the Senior Management Group may generate changes in the Plan.

5.2. Fiscal Year 2001

   a. **IT Program Objective #1:** Ensure that OIG, DoD, information systems and resources (automated and manual) support the overall mission needs and priorities of the organization.

      (1)   Evaluate Web-enabled applications. [OIG, DoD, Goal 1]

      (2)   Support the EDRMS Project. Ensure that the current hardware and software platforms are capable of handling the processing requirements and determine the software to be used. This will include the capability to store, retrieve, scan, and search text and graphics files for information. [OIG, DoD, Goal 1]

      (3)   Research applicability, costs and make recommendation on Document and Record Management System software for the OIG, DoD. [OIG, DoD, Goal 1]

      (4)   Extend capabilities of OIG, DoD, Intranet and Internet Web sites. Emphasize security, data presentation, stability, maintenance, and currency. [OIG, DoD, Goal 1]

      (5)   Continue conversion of OIG, DoD, applications to Web-based, to facilitate field office access. [OIG, DoD, Goal 1]

      (6)   Convert the Investigative Data System (IDS) and the Workhour Tracking System (WTS). [OIG, DoD, Goal 1]

      (7)   Convert the Automated Reports Tracking System (ARTS), the Departmental Inquiries (DI) system, and the Correspondence and Action Tracking System (CAATS) applications. [OIG, DoD, Goal 1]

      (8)   Perform systems development and maintenance as determined and prioritized by the functional components. [OIG, DoD, Goal 1]

      (9)   Research and evaluate the use of voice-input software. [OIG, DoD, Goal 1]

      (10)   Research and evaluate enhanced links to be provided via the Intranet. [OIG, DoD, Goal 1]

      (11)   Support major initiatives such as Civilian Health and Medical Program of the Uniformed Services (CHAMPUS), and TeamMate. [OIG, DoD, Goal 1]

      (12)   Complete an automated interface between *Travel Manager* and *Free Balance*. [OIG, DoD, Goal 1]

b. **IT Program Objective #2:** Promote integration of automated information through emphasis on standardization and/or compatibility of hardware, software, and data elements.

(1) Migrate to *Windows 2000*. [OIG, DoD, Goal 1]

(2) Update personal computer (PC) virus scanning software. [OIG, DoD, Goal 1]

(3) Migrate to *Office 2000*. [OIG, DoD, Goal 1]

(4) Upgrade Frame Relay sites. [OIG, DoD, Goal 1]

(5) Upgrade cabling. [OIG, DoD, Goal 1]

(6) Upgrade servers. [OIG, DoD, Goal 1]

(7) Upgrade pagers. [OIG, DoD, Goal 1]

(8) Analyze mix of hardware, such as desktops, notebooks, docking stations, and mobile computing devices. [OIG, DoD, Goal 1]

(9) Evaluate use of wireless Local Area Networks (LANs). [OIG, DoD, Goal 1]

(10) Evaluate need to upgrade *Citrix*. [OIG, DoD, Goal 1]

(11) Evaluate best way to enable field personnel to access forms and travel capabilities. [OIG, DoD, Goal 1]

(12) Evaluate best way to enable E-Mail routing for travel information. [OIG, DoD, Goal 1]

(13) Evaluate hardware trouble alert software. [OIG, DoD, Goal 1]

(14) Evaluate use of underutilized features of *Microsoft Outlook and Exchange*. [OIG, DoD, Goal 1]

(15) Evaluate use of Pentagon Global Address list. [OIG, DoD, Goal 1]

c. **IT Program Objective #3:** Ensure information is secure and available to authorized users.

(1) Complete the initial disaster recovery site setup. [OIG, DoD, Goals 1 and 2]

(2) Complete agreements, testing, and procedures for disaster recovery site. [OIG, DoD, Goal 1]

(3) Conduct a security assessment of DAMIS. [OIG, DoD, Goal 1]

(4) Maintain required Information Assurance (IA) certifications. [OIG, DoD, Goal 1]

(5) Implement PKI Team to serve as technical experts on how the PKI service will be technically implemented within the OIG, DoD. [OIG, DoD, Goal 1]

(6) Implement secure server capability for Intranet and obtain Web server certificates. [OIG, DoD, Goal 1]

(7)   Research and evaluate best way to send and receive encrypted documents. [OIG, DoD, Goal 1]

(8)   Research and evaluate use of Secure Telephone Equipment (STE) to replace current secure telephones. [OIG, DoD, Goal 1]

(9)   Research and evaluate classified video conferencing capability. [OIG, DoD, Goal 1]

(10)   Maintain classified LAN. {OIG, DoD, Goal 1]

(11)   Evaluate classified computer virus scanning software. [OIG, DoD, Goal 1]

(12)   Review classified communications software. [OIG, DoD, Goal 1]

(13)   Review utility software on classified systems. [OIG, DoD, Goal 1]

(14)   Maintain hardware and software to enable the OIG, DoD, to use INTELINK, classified E-Mail, and other classified services from the Joint Worldwide Intelligence System (JWICS) Sensitive Compartmented Information (SCI) network. [OIG, DoD, Goal 1]

(15)   Maintain hardware and software to enable the OIG, DoD, to use INTELINK-S, classified E-Mail, and other classified services from the Secret Internet Protocol Router Network (SIPRNET) collateral Secret network. [OIG, DoD, Goal 1]

(16)   Deploy PKI. [OIG, DoD, Goal 1]

(17)   Deploy E-Mail signature capability. [OIG, DoD, Goal 1]

(18)   Implement *Smart Gate*. [OIG, DoD, Goal 1]

(19)   Develop IT security plan. [OIG, DoD, Goal 1]

(20)   Complete system security authorization for IDS. [OIG, DoD, Goal 1]

(21)   Meet Section 508 requirements for use of systems by individuals with disabilities. [OIG, DoD, Goal 1]

(22)   Continue monitoring to detect inappropriate use of Government resources or intrusion from outside sources. [OIG, DoD, Goal 1]

(23)   Continue to upgrade virus scanning software. [OIG, DoD, Goal 1]

d.   **IT Program Objective #4:** Review and ensure compliance with internal and external guidelines.

(1)   Update 5-Year IT Plan and IT policies and directives. [OIG, DoD, Goal 2]

(2)   Evaluate OIG, DoD, data communications against DoD Defense Message System compliance. [OIG, DoD, Goal 2]

(3)   Review configuration management procedures. [OIG, DoD, Goal 2]

(4)   Review OIG, DoD, systems for compliance with the Electronic Records Management and Freedom of Information Act. [OIG, DoD, Goal 2]

    e. **IT Program Objective #5:** Ensure OIG, DoD, component involvement throughout the planning process.

    (1)   Ensure that OIG, DoD, components and ISD plan well in advance for major acquisitions and upgrades. [OIG, DoD, Goal 1]

    (2)   Conduct planning sessions with the OIG, DoD, components to determine their needs. [OIG, DoD, Goal 1]

    (3)   Provide briefings to, and obtain guidance from, the OIG, DoD Senior Management Group. [OIG, DoD, Goals 1 and 2]

    (4)   Visit field activities to evaluate needs. [OIG, DoD, Goals 1 and 2]

    f. **IT Program Objective #6:** Continue implementation of DoD-wide systems.

    (1)   Ensure adequate hardware and software support is available for migratory and DoD-wide systems. [OIG, DoD, Goal 1]

    (2)   Serve as the PSA for DoD-wide audit and criminal investigative functions. [OIG, DoD, Goals 1 and 2]

    (3)   Serve as the PSA for data standardization in assigned functional areas. [OIG, DoD, Goals 1and 2]

    g. **IT Program Objective #7:** Rapidly deploy appropriate advanced technology to support the mission.

    (1)   Evaluate deployment strategy for application software, to include off-the-shelf software. [OIG, DoD, Goal 1]

    (2)   Develop standard procedures and plans for development and deployment of new application systems and their maintenance. [OIG, DoD, Goal 1]

    (3)   Take full advantage of tools that will assist in rapidly conducting the analysis, documentation, development, and deployment of IT. The ISD, OA&IM, shall use commercially available software when available and where applicable. [OIG, DoD, Goal 1]

    (4)   Evaluate System Management Services to maintain an inventory of all IT resources and to deploy software in an automated fashion. [OIG, DoD, Goal 1]

    h. **IT Program Objective #8.** Develop ISD human capital.

    (1)   Plan for employees' professional growth. This may include certification, accountability, deliverables, and performance. [OIG, DoD, Goal 2]

    (2)   Evaluate when contractor workforce is the best way to support the mission and when use of Government employees is most effective. [OIG, DoD, Goal 2]

    (3)   Conduct annual Business Process Improvement Initiatives. [OIG, DoD, Goal 2]

    (4)   Evaluate Help Desk Institute requirements for certification of personnel. [OIG, DoD, Goal 2]

(5)   Evaluate rotational assignments for ISD personnel. [OIG, DoD, Goal 2]

5.3. <u>Fiscal Year 2002</u>

a. **IT Program Objective #1:** Ensure that OIG, DoD, information systems and resources (automated and manual) support the overall mission needs and priorities of the organization. [OIG, DoD, Goal 1]

(1)   Develop two additional IDS database modules needed to support the OAIG-INV reporting requirements. This will include converting the IDS to Web-based applications for Internet browser access by Headquarters and field activities. [OIG, DoD, Goal 1]

(2)   Research and evaluate best way to track commercial purchase card transactions. [OIG, DoD, Goal 1]

(3)   Research and evaluate best way to link *Travel Manager* to reservation system and travel information. [OIG, DoD, Goal 1]

(4)   Expand Web-enabled applications. [OIG, DoD, Goal 1]

(5)   Support the EDRMS project. Ensure that the current hardware and software platforms are capable of handling the processing requirements and determine the software to be used. This will include the capability to store, retrieve, scan, and search text and graphics files for information. [OIG, DoD, Goal 1]

(6)   Extend capabilities of OIG, DoD, Intranet and Internet Web sites. Emphasize security, data presentation, stability, maintenance, and currency. [OIG, DoD, Goal 1]

(7)   Perform systems development and maintenance as determined and prioritized by the functional components. [OIG, DoD, Goal 1]

(8)   Research and evaluate enhanced links to be provided via the Intranet. [OIG, DoD, Goal 1]

(9)   Migrate applications from Hewlett Packard servers (HP) to New Technology (NT). [OIG, DoD, Goal 1]

(10) Join the DoD Defense Automated Requisition Tracking System. (DARTS) effort.

b. **IT Program Objective #2:** Promote integration of automated information through an emphasis on standardization and/or compatibility of hardware, software, and data elements.

(1)   Manage life cycle of minicomputers. [OIG, DoD, Goal 1]

(2)   Evaluate telephone technologies. [OIG, DoD, Goal 1]

(3)   Evaluate virus-scanning software. [OIG, DoD, Goal 1]

(4)   Review and procure communications software. [OIG, DoD, Goal 1]

(5)   Evaluate life-cycle management of servers. [OIG, DoD, Goal 1]

(6)   Review LAN/Wide Area Network (WAN) performance. [OIG, DoD, Goal 1]

(7)   Research state-of-the-art configuration management and monitoring software for LAN/WAN. [OIG, DoD, Goal 1]

(8)   Research state-of-the-art technology for remote communications wide area or dial-in. [OIG, DoD, Goal 1]

(9)   Evaluate minicomputers based on fiscal year requirements. [OIG, DoD, Goal 1]

(10)   Research state-of-the-art voice communications. [OIG, DoD, Goal 1]

(11)   Research state-of-the-art LAN/WAN. [OIG, DoD, Goal 1]

(12)   Evaluate digital modems. [OIG, DoD, Goal 1]

(13)   Replace remaining HPs. [OIG, DoD, Goal 1]

c.   **IT Program Objective #3:** Ensure information is secure and available to authorized users.

(1)   Reevaluate hosting of DAMIS. [OIG, DoD, Goal 1]

(2)   Complete the disaster recovery site setup. [OIG, DoD, Goal 1]

(3)   Complete implementation procedures and testing for disaster recovery site. [OIG, DoD, Goal 1]

(4)   Maintain required IA certifications. [OIG, DoD, Goal 1]

(5)   Maintain classified LAN. {OIG, DoD, Goal 1]

(6)   Maintain hardware and software to enable the OIG, DoD, to use INTELINK, classified E-Mail, and other classified services from the JWICS SCI network. [OIG, DoD, Goal 1]

(7)   Maintain hardware and software to enable the OIG, DoD, to use INTELINK-S, classified E-Mail, and other classified services from the SIPRNET collateral Secret network. [OIG, DoD, Goal 1]

(8)   Train users on PKI. [OIG, DoD, Goal 1]

(9)   Deploy encrypted E-Mail. [OIG, DoD, Goal 1]

(10)   Deploy Local Registration Authority. [OIG, DoD, Goal 1]

(11)   Deploy PKI. [OIG, DoD, Goal 1]

(12)   Continue to meet Section 508 requirements for use of systems by individuals with disabilities. [OIG, DoD, Goal 1]

(13)   Continue monitoring to detect inappropriate use of Government resources or intrusion from outside sources. [OIG, DoD, Goal 1]

(14)   Continue to upgrade virus scanning software. [OIG, DoD, Goal 1]

d.   **IT Program Objective #4:** Review and ensure compliance with internal and external guidelines.

(1)   Update 5-Year IT Plan and IT policies and directives. [OIG, DoD, Goal 1]

(2)   Evaluate OIG, DoD, data communications against DoD Defense Message System compliance. [OIG, DoD, Goal 1]

(3)   Review configuration management procedures. [OIG, DoD, Goal 1]

(4)   Review OIG, DoD, systems for compliance with the Electronic Records Management and Freedom of Information Act. [OIG, DoD, Goal 1]

e.   **IT Program Objective #5:** Ensure component involvement throughout the planning process.

(1)   Support field office moves (10 - 12 per year). [OIG, DoD, Goal 1]

(2)   Ensure that OIG, DoD, components and ISD, OA&IM, plan ahead for major acquisitions and upgrades. [OIG, DoD, Goal 1]

(3)   Conduct planning sessions with the OIG, DoD, components and field offices to determine their needs. [OIG, DoD, Goals 1 and 2]

(4)   Provide briefings to, and obtain guidance from, the OIG, DoD Senior Management Group. [OIG, DoD, Goals 1 and 2]

f.   **IT Program Objective #6:** Continue implementation of DoD-wide systems.

(1)   Ensure adequate hardware and software support is available for migratory and DoD-wide systems. [OIG, DoD, Goal 1]

(2)   Serve as the PSA for DoD-wide audit and criminal investigative functions. [OIG, DoD, Goals 1 and 2]

(3)   Serve as the PSA for data standardization in assigned functional areas. [OIG, DoD, Goals 1 and 2]

g.   **IT Program Objective #7:** Rapidly deploy appropriate advanced technology to support the mission.

(1)   Review deployment strategy for AIS applications. [OIG, DoD, Goal 1]

(2)   As an IT organization, the ISD, OA&IM, shall take full advantage of tools that will help in rapidly conducting the analysis, documentation, development, and deployment. The ISD, OA&IM, shall use commercially available software when available and where applicable. [OIG, DoD, Goal 1]

h.   **IT Program Objective #8:** Develop ISD human capital. Plan for employees' professional growth. This may include certification, accountability, deliverables, and performance. [OIG, DoD, Goal 2]

5.4.   Fiscal Year 2003

a.   **IT Program Objective #1:** Ensure that OIG, DoD, information systems and resources (automated and manual) support the overall mission needs and priorities of the OIG, DoD.

(1)   Support approved projects. Ensure that the current hardware and software platform is capable of handling the processing requirements and determine the software to be used. [OIG, DoD, Goal 1]

(2)   Continue to improve OIG, DoD, Intranet and Internet Web sites. Emphasize security, data presentation, stability, maintenance, and currency. [OIG, DoD, Goal 1]

(3)   Consolidate all IDS modules into an OAIG-INV "agent desktop" configuration for the collection, entry, modification, analysis, and reporting of data in support of the systems. [OIG, DoD, Goal 1]

(4)   Expand Web-enabled applications. [OIG, DoD, Goal 1]

(5)   Support the EDRMS project. Ensure that the current hardware and software platforms are capable of handling the processing requirements and determine the software to be used. This will include the capability to store, retrieve, scan, and search text and graphics files for information. [OIG, DoD, Goal 1]

(6)   Extend capabilities of OIG, DoD, Intranet and Internet Web sites. Emphasize security, data presentation, stability, maintenance, and currency. [OIG, DoD, Goal 1]

(7)   Perform systems development and maintenance as determined and prioritized by the functional components. [OIG, DoD, Goal 1]

(8)   Research and evaluate enhanced links to be provided via the Intranet. [OIG, DoD, Goal 1]

(9)   Perform yearly tests at disaster recovery site. [OIG, DoD, Goal 1]

b. **IT Program Objective #2:** Promote integration of automated information through an emphasis on standardization and/or compatibility of hardware, software, and data elements.

(1)   Review LAN/WAN operating system. [OIG, DoD, Goal 1]

(2)   Evaluate WAN equipment criteria for life-cycle management. [OIG, DoD, Goal 1]

(3)   Manage life cycle of minicomputers. [OIG, DoD, Goal 1]

(4)   Evaluate telephone technologies. [OIG, DoD, Goal 1]

(5)   Evaluate personal computing device operating system platform. [OIG, DoD, Goal 1]

(6)   Evaluate virus-scanning software. [OIG, DoD, Goal 1]

(7)   Review and procure communications software. [OIG, DoD, Goal 1]

(8)   Evaluate life-cycle management of servers. [OIG, DoD, Goal 1]

(9)   Review LAN/WAN performance. [OIG, DoD, Goal 1]

(10)   Research state-of-the-art configuration management and monitoring software for LAN/WAN. [OIG, DoD, Goal 1]

(11) Research state-of-the-art technology for remote communications wide area or dial-in. [OIG, DoD, Goal 1]

(12) Evaluate minicomputer performance. [OIG, DoD, Goal 1]

(13) Research state-of-the-art voice communication. [OIG, DoD, Goal 1]

(14) Research state-of-the-art LAN/WAN. [OIG, DoD, Goal 1]

(15) Research state-of-the-art scanning and imaging technology. [OIG, DoD, Goal 1]

c. **IT Program Objective #3:** Ensure information is secure and available to authorized users.

(1) Conduct a security assessment of OIG, DoD, systems. [OIG, DoD, Goal 1]

(2) Maintain required IA certifications. [OIG, DoD, Goal 1]

(3) Ensure adequate hardware and software support is available for effective use by the OIR. [OIG, DoD, Goal 1]

(4) Maintain classified LAN. [OIG, DoD, Goal 1]

(5) Review classified computer virus scanning software. [OIG, DoD, Goal 1]

(6) Review classified communications software. [OIG, DoD, Goal 1]

(7) Review utility software on classified systems. [OIG, DoD, Goal 1]

(8) Review secure telephone system requirements. [OIG, DoD, Goal 1]

(9) Maintain hardware and software to enable the OIG, DoD, to use INTELINK, classified E-Mail, and other classified services from the JWICS SCI network. [OIG, DoD, Goal 1]

(10) Maintain hardware and software to enable the OIG, DoD, to use INTELINK-S, classified E-Mail, and other classified services from the SIPRNET collateral Secret network. [OIG, DoD, Goal 1]

(11) Maintain capabilities of disaster recovery site. [OIG, DoD, Goal 1]

(12) Update documentation of disaster recovery records and procedures. [OIG, DoD, Goal 1]

d. **IT Program Objective #4:** Review and ensure compliance with internal and external guidelines.

(1) Review configuration management procedures. [OIG, DoD, Goal 1]

(2) Update 5-Year Plan and IT policies and directives. [OIG, DoD, Goal 1]

(3) Review OIG, DoD, systems for compliance with the Electronic Records Management, Section 508, and Freedom of Information Act. [OIG, DoD, Goal 1]

e. **IT Program Objective #5:** Ensure OIG, DoD, component involvement throughout the planning process.

(1)   Support field office moves (10 - 12 per year). [OIG, DoD, Goal 1]

(2)   Ensure that OIG, DoD, components and ISD, OA&IM, plan ahead for major acquisitions and upgrades. [OIG, DoD, Goal 1]

(3)   Conduct planning sessions with the OIG, DoD, components and field offices to determine their needs. [OIG, DoD, Goals 1 and 2]

(4)   Provide briefings to, and obtain guidance from, the OIG, DoD Senior Management Group. [OIG, DoD, Goals 1 and 2]

f.   **IT Program Objective #6:** Continue implementation of DoD-wide systems.

(1)   Ensure adequate hardware and software support is available for DoD-wide systems. [OIG, DoD, Goal 1]

(2)   Serve as the PSA for DoD-wide audit and criminal investigative functions. [OIG, DoD, Goals 1 and 2]

(3)   Serve as the PSA for data standardization in assigned functional areas. [OIG, DoD, Goals 1 and 2]

g.   **IT Program Objective #7:** Rapidly deploy appropriate advanced technology to support the mission.

(1)   Review deployment strategy for AIS applications. [OIG, DoD, Goal 1]

(2)   Take full advantage of tools that will help the OIG, DoD, to rapidly conduct the analysis, documentation, development, and deployment. The ISD, OA&IM, shall use commercially available software when available and where applicable. [OIG, DoD, Goal 1]

h.   **IT Program Objective #8:** Develop ISD human capital. Plan for employees' professional growth. This may include certification, accountability, deliverables, and performance. [OIG, DoD, Goal 2]

5.5.   Fiscal Year 2004

a.   **IT Program Objective #1:** Ensure that OIG, DoD, information systems and resources (automated and manual) support the overall mission needs and priorities of the OIG, DoD.

(1)   Support approved projects. Ensure that the current hardware and software platform is capable of handling the processing requirements and determine the software to be used. [OIG, DoD, Goal 1]

(2)   Continue to improve OIG, DoD, Intranet and Internet Web sites. Emphasize security, data presentation, stability, maintenance, and currency. [OIG, DoD, Goal 1]

(3)   Expand Web-enabled applications. [OIG, DoD, Goal 1]

(4)   Support the EDRMS project. Ensure that the current hardware and software platforms are capable of handling the processing requirements and determine the software to be used. This will include the capability to store, retrieve, scan, and search text and graphics files for information. [OIG, DoD, Goal 1]

(5)   Extend capabilities of OIG, DoD, Intranet and Internet Web sites. Emphasize security, data presentation, stability, maintenance, and currency. [OIG, DoD, Goal 1]

(6)   Perform systems development and maintenance as determined and prioritized by the functional components. [OIG, DoD, Goal 1]

(7)   Research and evaluate enhanced links to be provided via the Intranet. [OIG, DoD, Goal 1]

(8)   Perform yearly tests at disaster recovery site. [OIG, DoD, Goal 1]

b. **IT Program Objective #2:** Promote integration of automated information through an emphasis on standardization and/or compatibility of hardware, software, and data elements.

(1)   Review LAN/WAN operating system. [OIG, DoD, Goal 1]

(2)   Evaluate WAN equipment criteria for life-cycle management. [OIG, DoD, Goal 1]

(3)   Manage life cycle of minicomputers. [OIG, DoD, Goal 1]

(4)   Evaluate telephone technologies. [OIG, DoD, Goal 1]

(5)   Evaluate personal computing device operating system platform. [OIG, DoD, Goal 1]

(6)   Evaluate virus-scanning software. [OIG, DoD, Goal 1]

(7)   Review and procure communications software. [OIG, DoD, Goal 1]

(8)   Evaluate life-cycle management of servers. [OIG, DoD, Goal 1]

(9)   Review LAN/WAN performance. [OIG, DoD, Goal 1]

(10)   Research state-of-the-art configuration management and monitoring software for LAN/WAN. [OIG, DoD, Goal 1]

(11)   Research state-of-the-art technology for remote communications wide area or dial-in. [OIG, DoD, Goal 1]

(12)   Evaluate minicomputer performance. [OIG, DoD, Goal 1]

(13)   Research state-of-the-art voice communication. [OIG, DoD, Goal 1]

(14)   Research state-of-the-art LAN/WAN. [OIG, DoD, Goal 1]

(15)   Research state-of-the-art scanning and imaging technology. [OIG, DoD, Goal 1]

c. **IT Program Objective #3:** Ensure information is secure and available to authorized users.

(1)   Conduct a security assessment of OIG, DoD, systems. [OIG, DoD, Goal 1]

(2)   Maintain required IA certifications. [OIG, DoD, Goal 1]

(3)   Ensure adequate hardware and software support is available for effective use by the OIR. [OIG, DoD, Goal 1]

(4)   Maintain classified LAN.

(5)   Review classified computing device virus scanning software. [OIG, DoD, Goal 1]

(6)   Review classified communications software. [OIG, DoD, Goal 1]

(7)   Review utility software on classified systems. [OIG, DoD, Goal 1]

(8)   Review secure telephone system requirements. [OIG, DoD, Goal 1]

(9)   Maintain hardware and software to enable the OIG, DoD, to use INTELINK, classified E-Mail, and other classified services from the JWICS SCI network. [OIG, DoD, Goal 1]

(10)   Maintain hardware and software to enable the OIG, DoD, to use INTELINK-S, classified E-Mail, and other classified services from the SIPRNET collateral Secret network. [OIG, DoD, Goal 1]

(11)   Manage the upgrade of the JWICS circuit to Asynchronous Transfer Mode (ATM) capability. Consider adding a Top Secret SCI video teleconferencing (VTC) system when the circuit is upgraded to ATM. [OIG, DoD, Goal 1]

(12)   Maintain capabilities of disaster recovery site. [OIG, DoD, Goal 1]

(13)   Update documentation of disaster recovery records and procedures. [OIG, DoD, Goal 1]

d. **IT Program Objective #4:** Review and ensure compliance with internal and external guidelines.

(1)   Review configuration management procedures. [OIG, DoD, Goal 1]

(2)   Update 5-Year Plan and IT policies and directives. [OIG, DoD, Goal 1]

(3)   Review OIG, DoD, systems for compliance with the Electronic Records Management, Section 508, and Freedom of Information Act. [OIG, DoD, Goal 1]

e. **IT Program Objective #5:** Ensure OIG, DoD, component involvement throughout the planning process.

(1)   Support field office moves (10 - 12 per year). [OIG, DoD, Goal 1]

(2)   Ensure that OIG, DoD, components and ISD, OA&IM, plan ahead for major acquisitions and upgrades. [OIG, DoD, Goal 1]

(3)   Conduct planning sessions with the OIG, DoD, components and field offices to determine their needs. [OIG, DoD, Goals 1 and 2]

(4)   Provide briefings to, and obtain guidance from, the OIG, DoD Senior Management Group. [OIG, DoD, Goals 1 and 2]

f. **IT Program Objective #6:** Continue implementation of DoD-wide systems.

(1)   Ensure adequate hardware and software support is available for DoD-wide systems. [OIG, DoD, Goal 1]

(2)   Serve as the PSA for DoD-wide audit and criminal investigative functions. [OIG, DoD, Goals 1 and 2]

(3)   Serve as the PSA for data standardization in assigned functional areas. [OIG, DoD, Goals 1 and 2]

g.   **IT Program Objective #7:** Rapidly deploy appropriate advanced technology to support the mission.

(1)   Review deployment strategy for AIS applications. [OIG, DoD, Goal 1]

(2)   Take full advantage of tools that will help the OIG, DoD, to rapidly conduct the analysis, documentation, development, and deployment. The ISD, OA&IM, shall use commercially available software when available and where applicable. [OIG, DoD, Goal 1]

h.   **IT Program Objective #8:** Develop ISD human capital. Plan for employees' professional growth. This may include certification, accountability, deliverables, and performance. [OIG, DoD, Goal 2]

5.6.   <u>Fiscal Year 2005</u>

a.   **IT Program Objective #1:** Ensure that OIG, DoD, information systems and resources (automated and manual) support the overall mission needs and priorities of the OIG, DoD.

(1)   Support approved projects. Ensure that the current hardware and software platform is capable of handling the processing requirements and determine the software to be used. [OIG, DoD, Goal 1]

(2)   Continue to improve OIG, DoD, Intranet and Internet Web sites. Emphasize security, data presentation, stability, maintenance, and currency. [OIG, DoD, Goal 1]

(3)   Expand Web-enabled applications. [OIG, DoD, Goal 1]

(4)   Support the EDRMS project. Ensure that the current hardware and software platforms are capable of handling the processing requirements and determine the software to be used. This will include the capability to store, retrieve, scan, and search text and graphics files for information. [OIG, DoD, Goal 1]

(5)   Extend capabilities of OIG, DoD, Intranet and Internet Web sites. Emphasize security, data presentation, stability, maintenance, and currency. [OIG, DoD, Goal 1]

(6)   Perform systems development and maintenance as determined and prioritized by the functional components. [OIG, DoD, Goal 1]

(7)   Research and evaluate enhanced links to be provided via the Intranet. [OIG, DoD, Goal 1]

(8)   Perform yearly tests at disaster recovery site. [OIG, DoD, Goal 1]

b.   **IT Program Objective #2:** Promote integration of automated information through an emphasis on standardization and/or compatibility of hardware, software, and data elements.

(1)   Review LAN/WAN operating system. [OIG, DoD, Goal 1]

(2)   Evaluate WAN equipment criteria for life-cycle management. [OIG, DoD, Goal 1]

(3)   Manage life cycle of minicomputers. [OIG, DoD, Goal 1]

(4)   Evaluate telephone technologies. [OIG, DoD, Goal 1]

(5)   Evaluate personal computing device operating system platform. [OIG, DoD, Goal 1]

(6)   Evaluate virus-scanning software. [OIG, DoD, Goal 1]

(7)   Review and procure communications software. [OIG, DoD, Goal 1]

(8)   Evaluate life-cycle management of servers. [OIG, DoD, Goal 1]

(9)   Review LAN/WAN performance. [OIG, DoD, Goal 1]

(10)   Research state-of-the-art configuration management and monitoring software for LAN/WAN. [OIG, DoD, Goal 1]

(11)   Research state-of-the-art technology for remote communications wide area or dial-in. [OIG, DoD, Goal 1]

(12)   Evaluate minicomputer performance. [OIG, DoD, Goal 1]

(13)   Research state-of-the-art voice communication. [OIG, DoD, Goal 1]

(14)   Research state-of-the-art LAN/WAN. [OIG, DoD, Goal 1]

(15)   Research state-of-the-art scanning and imaging technology. [OIG, DoD, Goal 1]

(16)   Upgrade intrusion detection hardware and software. [OIG, DoD, Goal 1]

   c.   **IT Program Objective #3:** Ensure information is secure and available to authorized users.

(1)   Conduct a security assessment of OIG, DoD, systems. [OIG, DoD, Goal 1]

(2)   Maintain required IA certifications. [OIG, DoD, Goal 1]

(3)   Ensure adequate hardware and software support is available for effective use by the OIR. [OIG, DoD, Goal 1]

(4)   Maintain classified LAN. [OIG, DoD, Goal 1]

(5)   Review classified computing device virus scanning software. [OIG, DoD, Goal 1]

(6)   Review classified communications software. [OIG, DoD, Goal 1]

(7)   Review utility software on classified systems. [OIG, DoD, Goal 1]

(8)   Review secure telephone system requirements. [OIG, DoD, Goal 1]

(9)   Maintain hardware and software to enable the OIG, DoD, to use INTELINK, classified E-Mail, and other classified services from the JWICS SCI network. [OIG, DoD, Goal 1]

       (10)   Maintain hardware and software to enable the OIG, DoD, to use INTELINK-S, classified E-Mail, and other classified services from the SIPRNET collateral Secret network. [OIG, DoD, Goal 1]

       (11)   Maintain capabilities of disaster recovery site. [OIG, DoD, Goal 1]

       (12)   Update documentation of disaster recovery records and procedures. [OIG, DoD, Goal 1]

    d. **IT Program Objective #4:** Review and ensure compliance with internal and external guidelines.

       (1)   Review configuration management procedures. [OIG, DoD, Goal 1]

       (2)   Update 5-Year Plan and IT policies and directives. [OIG, DoD, Goal 1]

       (3)   Review OIG, DoD, systems for compliance with the Electronic Records Management, Section 508, and Freedom of Information Act. [OIG, DoD, Goal 1]

    e. **IT Program Objective #5:** Ensure component involvement throughout the planning process.

       (1)   Support field office moves (10 - 12 per year). [OIG, DoD, Goal 1]

       (2)   Ensure that OIG, DoD, components and ISD, OA&IM, plan ahead for major acquisitions and upgrades. [OIG, DoD, Goal 1]

       (3)   Conduct planning sessions with the OIG, DoD, components and field offices to determine their needs. [OIG, DoD, Goals 1 and 2]

       (4)   Provide briefings to, and obtain guidance from, the OIG, DoD Senior Management Group. [OIG, DoD, Goals 1 and 2]

    f. **IT Program Objective #6:** Continue implementation of DoD-wide systems.

       (1)   Ensure adequate hardware and software support is available for DoD-wide systems. [OIG, DoD, Goal 1]

       (2)   Serve as the PSA for DoD-wide audit and criminal investigative functions. [OIG, DoD, Goals 1 and 2]

       (3)   Serve as the PSA for data standardization in assigned functional areas. [OIG, DoD, Goals 1 and 2]

    g. **IT Program Objective #7:** Rapidly deploy appropriate advanced technology to support the mission.

       (1)   Review deployment strategy for AIS applications. [OIG, DoD, Goal 1]

       (2)   Take full advantage of tools that will help the OIG, DoD, to rapidly conduct the analysis, documentation, development, and deployment. The ISD, OA&IM, shall use commercially available software when available and where applicable. [OIG, DoD, Goal 1]

    h. **IT Program Objective #8:** Develop ISD human capital. Plan for employees' professional growth. This may include certification, accountability, deliverables, and performance. [OIG, DoD, Goal 2]

APPENDIX A
REFERENCES

a.   Inspector General, Department of Defense, Strategic Plan 2001-2005, June 2001

b.   The Privacy Act of 1974, as amended

c.   Information Management (IM) Strategic Plan Version 2.0, October 1999, Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)

d.   Appendix 3 of title 31, United States Code, Inspector General Act of 1978, as amended

e.   DoD Directive 5106.1, "Inspector General of the Department of Defense," January 4, 2001

APPENDIX B
ACRONYMS

AIS	Automated Information System
ARTS	Automated Reports Tracking System
ASD	Assistant Secretary of Defense
ATM	Asynchronous Transfer Mode
BPR	Business Process Reengineering
C3I	Command, Control, Communications, and Intelligence
CAATS	Correspondence and Action Tracking System
CHAMPUS	Civilian Health and Medical Program of the Uniformed Services
DAMIS	Defense Audit Management Information System
DARTS	Defense Automated Requisition Tracking System
DI	Departmental Inquiries
DoD	Department of Defense
HP	Hewlett Packard
IA	Information Assurance
IDS	Investigative Data System
ISD	Information System Directorate
IT	Information Technology
JWICS	Joint Worldwide Intelligence Communications System
LAN	Local Area Network
NT	New Technology
OA&IM	Office of Administration and Information Management
OAIG-AUD	Office of the Assistant Inspector General for Auditing
OAIG-INV	Office of the Assistant Inspector General for Investigations
OIG	Office of the Inspector General
OIR	Office of Intelligence Review
PC	Personal Computer
PKI	Public Key Infrastructure
PPBS	Planning, Programming and Budgeting System
PSA	Principal Staff Assistant

SIPRNET	Secret Internet Protocol Router Network
STE	Secure Telephone Equipment
VTC	Video Teleconference
WAN	Wide Area Network
WTS	Workhour Tracking System